

What is claimed is:

1           1.    A method for replacing an existing authentication  
2    keying variable K with a new authentication keying variable  
3    K' generated from K, the method comprising:

4           generating a first authentication word,  $W_1$ , based on  
5    the existing keying variable K, a counter, C, and a master  
6    keying variable, KM;

7           selecting a portion of  $W_1$  as a first portion of K'; and  
8           completing remaining portions of K' by iteratively:

9           generating new authentication words,  $W_n$  based on  
10    C, KM, and a concatenation of a prior authentication  
11    word and K; and

12           selecting an additional portion of  $W_n$  as an  
13    additional portion of K'.

1           2.    The method of claim 1, wherein generating new  
2    authentication words,  $W_n$ , comprises generating new  
3    authentication words based on C, KM, and a concatenation of  
4    an immediately prior authentication word  $W_{n-1}$  and K.

1           3.    The method of claim 1, wherein K' is different in  
2    length than K.

1           4.    The method of claim 1, wherein K' is equal in  
2    length to K.

1           6.    The method of claim 1, wherein selecting a  
2   portion of  $W_1$  comprises selecting 8-bits of  $W_1$ .

1           8.    The method of claim 1, wherein selecting an  
2   additional portion of  $W_n$  as an additional portion of  $K'$   
3   comprises selecting the first 8-bits of  $W_n$  as  $n^{th}$  8-bits of  
4    $K'$ .

3           a processing circuit; and

7           generating a first authentication word,  $W_1$ , based  
8       on the existing keying variable  $K$ , a counter,  $C$ , and a  
9       master keying variable,  $KM$ ;

11 K'; and

17           selecting an additional portion of  $W_n$  as an  
18           additional portion of  $K'$ .

1        11. The replacement authentication key generator of  
2        claim 9, wherein  $K'$  is different in length than  $K$ .

1           13. The replacement authentication key generator of  
2   claim 9, wherein the instructions for selecting a portion  
3   of  $W_1$  comprises selecting 8-bits of  $W_1$ .

1        14. The replacement authentication key generator of  
2        claim 13, wherein the instructions for selecting a portion  
3        of  $W_1$  comprises selecting the first 8-bits of  $W_1$ .

1        15. The replacement authentication key generator of  
2 claim 9, wherein the instructions for selecting an  
3 additional portion of  $W_n$  as an additional portion of  $K'$   
4 comprises selecting the first 8-bits of  $W_n$  as  $n^{\text{th}}$  8-bits of  
5  $K'$ .

1        16. In an appliance communication network, a method  
2 for authenticating appliance messages, the method  
3 comprising:

4        maintaining at an appliance communication center a  
5 shared message counter, the shared message counter shared  
6 between the communication center and a remotely located  
7 appliance;

8        applying an appliance message and the shared message  
9 counter, as stored in the communication center, to an  
10 authentication algorithm to generate a first authentication  
11 word; and

12        transmitting the appliance message and the first  
13 authentication word as an authenticated message to the  
14 appliance.

1        17. The method of claim 16, further comprising:

2        receiving the authenticated message at the appliance;

3 applying the shared message counter, as stored in the  
4 appliance, and the appliance message to the authentication  
5 algorithm to generate a second authentication word; and

6 comparing the first authentication word and the second  
7 authentication word to determine authenticity of the  
8 authenticated message.

1 18. The method of claim 17, further comprising  
2 incrementing the shared message counter, as stored in the  
3 appliance, after receiving a genuine authenticated message  
4 at the appliance.

1 19. The method of claim 16, wherein applying  
2 comprises applying an authentication keying variable, K.

1 20. The method of claim 19, wherein applying  
2 comprises:

3 establishing a working register R, comprising at least  
4 bytes R0, R1, R2, R3;

5 initializing R3 to a directional code, representing a  
6 transmission from the appliance communication center to the  
7 appliance;

8 initializing at least R2, R1, and R0 to the bytes C2,  
9 C1, and C0 of the shared message counter, as stored in the  
10 communication center, respectively;

11           iteratively performing, a first number of times, the  
12 steps of:  
13           performing at least one arithmetic, logical and  
14           shifting operation on R;  
15           shifting R; and  
16           setting the first authentication word equal to the  
17 value contained in R.

1           21. The method of claim 20, wherein performing a  
2 transformation of R comprises iteratively performing, as  
3 many times as there are bytes in K, the steps of:

4           establishing an index, equal to the greater of:  
5           a non-zero constant; and  
6           a number of bytes in the message less one;  
7           and  
8           iteratively performing, a number of times equal  
9 to the index plus one:

10           forming P as the dot product of R2 and R0;  
11           forming Q as the bitwise exclusive or of P  
12 with the constant expression '01010101';  
13           forming S by adding Q to K;  
14           forming S' by end around rotating S;  
15           forming T as the bitwise exclusive or of S'  
16 and R3;

17                   forming F as the bitwise exclusive or of T  
18                   with a byte of the appliance message; and  
19                   replacing R3 with R2, R2 with R1, R1 with  
20                   R0, and R0 with F.

1           22. The method of claim 21, wherein the non-zero  
2           constant is at least 3.

1           23. The method of claim 16, wherein maintaining  
2           comprises maintaining a separate shared counter for a  
3           plurality of appliances.

1           24. The method of claim 16, further comprising  
2           incrementing the shared message counter, as stored in the  
3           communication center, after transmitting the authenticated  
4           message to the appliance.

1           25. An appliance communication center comprising:  
2           network connections terminating at appliances;  
3           a processing circuit;  
4           a memory storing a plurality of shared counters, each  
5           shared counter shared between the communication center and  
6           an appliance, the memory further storing instructions for:  
7                 maintaining at an appliance communication center  
8                 a shared message counter, the shared message counter

9 shared between the communication center and a remotely  
10 located appliance;

11 applying an appliance message and the shared  
12 message counter, as stored in the communication  
13 center, to an authentication algorithm to generate a  
14 first authentication word; and

15 transmitting the appliance message and the first  
16 authentication word as an authenticated message to the  
17 appliance.

1 26. The appliance communication center of claim 25,  
2 wherein the instructions for maintaining comprises  
3 maintaining a separate shared counter for a plurality of  
4 appliances.

1 27. The appliance communication center of claim 25,  
2 wherein the instructions further comprise incrementing the  
3 shared message counter, as stored in the communication  
4 center, after transmitting the authenticated message to the  
5 appliance.

1 28. In an appliance, an appliance message  
2 authentication device comprising:

3 a processor; and

4 a memory coupled to the processor, the memory storing  
5 instructions for execution by the processor for:



8           applying the shared message counter, as stored in  
9           the appliance, and the appliance message to the  
10          authentication algorithm to generate a second  
11          authentication word; and

1        29. The appliance message authentication device of  
2        claim 28, wherein the instructions further comprise  
3        incrementing the shared message counter, as stored in the  
4        appliance, after receiving a genuine authenticated message  
5        at the appliance.

4       maintaining at an appliance a shared message counter,  
5       the shared message counter shared between the appliance and  
6       a remotely located appliance communication center;

-37-

10       transmitting the appliance message and the first  
11 authentication word as an authenticated message to the  
12 appliance communication center.

1       31. The method of claim 30, further comprising:  
2       receiving the authenticated message at the appliance  
3 communication center;  
4       applying the shared message counter, as stored in the  
5 appliance communication center, and the appliance message  
6 to the authentication algorithm to generate a second  
7 authentication word; and  
8       comparing the first authentication word and the second  
9 authentication word to determine authenticity of the  
10 authenticated message.